

REMARKS

The Applicants request reconsideration of the rejection.

Claims 1, 3 and 28 are now pending, including new claim 28.

The Examiner objected to the specification as failing to provide proper antecedent basis for the limitation wherein said input data D1 does not have a constant Hamming weight. The claims have been amended to remove reference to the input data D1 not having a constant Hamming weight. The Applicants make no admission as to the propriety of the objection.

Claims 1-8 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement, the Examiner again citing the limitation wherein said input data D1 does not have a constant Hamming weight. The cancellation of this language from the claims avoids the rejection, although the Applicants make no admission as to its propriety.

Claims 1-8, 18, 20-22 and 24-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the applicants admitted prior art (AAPA) in view of Jaffe et al., U.S. Patent No. 6,510,518 (Jaffe). The Applicants traverse these rejections as follows.

As amended, independent claim 1 recites an information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2. The information-processing apparatus comprises a memory holding a table of candidates of disturbance data XI which maintains a constant Hamming weight before and after performing the predetermined processing OP1 using the disturbance data XI; a selector for selecting the disturbance data XI

from the table; and a disturbance data processing means for performing the predetermined processing OP1 by using the disturbance data XI selected from the table by the selector, thereby generating disturbance data XO.

These amendments to claim 1, and particularly the amendment requiring the disturbance data XI to maintain a constant Hamming weight before and after the processing thereof in the predetermined processing OP1, prevents the disturbance data XI from becoming equal to either of the values 0 or 8 when the disturbance data XI is processed by the predetermined processing OP1 to thereby generate the disturbance data XO, which is thereafter used in an inverse-transformation processing OP2 on data H2 to thereby generate the processed data D2. Moreover, by the functions performed by the information-processing apparatus as set forth in claim 1, the processing OP1 and the disturbance data are substantially undetectable by observing the waveform of the current consumption.

Parenthetically, the predetermined processing OP1 set forth in the claims may be represented by the function f as set forth in the specification.

Turning to the secondary reference to Jaffe, this patent broadly states that a constant Hamming weight representation of data is used in internal operations (col. 4, lines 56-67). The Applicants submit that using a constant Hamming weight representation of data means that some signal or signals are applied to data to obtain a constant Hamming weight representation of that data. See, for example, Jaffe at col. 5, lines 9-11: "A simple constant Hamming weight representation maps 'one' onto the two-digit binary number 10, and 'zero' onto 01." Other constant Hamming weight representations follow.

In order to attempt a combination of AAPA with Jaffe, it is necessary to apply Jaffe's "constant Hamming weight representation" to input data of AAPA. By doing so, twice the data (including the data added by Jaffe's method) must be processed. In order to process twice the data, at least twice the scale or size of the circuit must be provided. Therefore, the combination asserted in the Office Action is counterintuitive to the person of ordinary skill in the art because such represents a significant disadvantage in practical use. That is, finding the space for mounting the large scale or large size circuit in the AAPA device would be difficult and thus not considered by the person of ordinary skill in the art.

The apparatus set forth in claim 1, on the other hand, does not require the increase in the size or scale of the circuit, because the table of candidates of disturbance data XI stored in the memory, selecting the disturbance data XI from the table, and generating disturbance data XO from the disturbance data XI, are sufficient to disturb the input data D1 to provide disturbance data XO in a process OP2 performed on transformed data H2 to obtain processed data D2 without requiring a processing of 2x the data using a larger sized and larger scale circuit.

In addition, the Applicants note that neither the disturbance data XI nor the disturbance data XO is obtained by using the first and second disturbance data of AAPA and a constant Hamming weight representation as taught by Jaffe. If the first and second disturbance data of AAPA are applied by a constant Hamming weight representation taught by Jaffe, the second disturbance data obtained by using a processing operation on the first disturbance data of AAPA may not securely prevent the Hamming weight of disturbance data XI from becoming 0 or 8, which leaves a

potential security hole in the attempt to prevent inference of the processing and secret key by observation of the waveform of the current consumption.

In view of the above, the Applicants respectfully submit that independent claim 1 is patentably distinguishable from any combination of AAPA and Jaffe that would be considered by the person of ordinary skill in the art.

Dependent claim 3 requires each bit of the processed disturbance data XO and the disturbance data XI to have a logic value of 0 or 1 at a probability of 50%. As set forth in paragraph [0086] of the published U.S. Patent Application 2002/0154767, requiring the disturbance data XO and XI to have this logic value specifically is a preferred embodiment for making difficult to identify the disturbance data from the waveform of the current consumed during processing of the disturbance data.

New independent claim 28 can be distinguished similarly. Claim 28 recites an information-processing apparatus that comprises a memory holding a table of candidate pairs of disturbance data XI, XO, wherein the disturbance data XI maintains a constant Hamming weight before and after processing thereof with the predetermined processing OP1, and wherein disturbance data XO is obtained from processing the disturbance data XI with the predetermined processing OP1.

Claim 28 also recites a selector for selecting a pair of disturbance data from the table, a data transform means for transforming the input data D1 using the disturbance data XI of the selected pair to generate transforming data H1; the transformed-data-processing means for carrying out the predetermined processing OP1 or a different processing, on the transformed data H1 in order to generate processed transformed data H2; and a data inverse-transform means for carrying out

inverse-transformation processing OP2 on the processed transformed data H2 using the disturbance data XO of the selected pair, in order to generate processed data D2. Accordingly, for reasons similar to those advanced above, claim 28 is patentably distinguishable from Jaffe.

The remaining claims have been canceled without any admission to the propriety of the outstanding rejection. Accordingly, the Applicants submit that claims 1, 3 and 28 are patentably distinguishable over Jaffe, and that a Notice of Allowance should be issued.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Brundidge & Stanger, P.C., Deposit Account No. 50-4888 (referencing attorney docket no. NIT-295).

Respectfully submitted,

BRUNDIDGE & STANGER, P.C.

/Daniel J. Stanger/
Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1470